Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Honeypot v prostředí IP telefonie

Honeypot in IP Telephony

2014 **Zuzana Bajáková**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Zuzana Bajáková**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Honeypot v prostředí IP telefonie
Honeypot in IP Telephony

Zásady pro vypracování:

Bezpečnost IP telefonie na protokolu SIP je v současnosti často řešeným tématem a uspokojivé řešení této problematiky vyžaduje dostatečné informace o chování útočníka. Tyto informace se dají získávat pomocí Honeypotů, které jsou k těmto účelům přímo navrženy. Cílem práce je proto vytvořit komplexní analýzu dostupných Honeypotů pro IP telefonii a protokol SIP, podrobit je praktickému testování a navrhnout ten nejvhodnější pro využití v praxi.

Body zadání:
1. Studijní část: Bezpečnostní rizika ve VoIP SIP telefonii, problematika Honeypotů.
2. Detailní přehled nástrojů pro realizaci Honeypotů v IP telefonii.
3. Praktická realizace a implementace vybraných Honeypotů a jejich nasazení v SIP infrastruktuře.
4. Analýza výsledků funkčnosti a použitelnosti Honeypotů pro praktický provoz.
5. Teoretický návrh a zapojení vhodného Honeypotu pro využití v praxi.

Seznam doporučené odborné literatury:

[1] Virtual Honeypots: From Botnet Tracking to Intrusion Detection - Niels Provos, Thorsten Holz , ISBN: 978-0321336323
[2] Honeypots: Tracking Hackers - Lance Spitzner , ISBN: 978-0321108951

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Filip Řezáč**

Datum zadání: 16.11.2012
Datum odevzdání: 07.05.2014

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

VYSOKÁ ŠKOLA BÁŇSKÁ - TECHNICKÁ UNIVERZITA OSTRAVA Fakulta elektrotechniky a informatiky

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení: Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně. Uvedla jsem všechny literární prameny a publikace, ze kterých jsem čerpala.

V Ostravě dne: 29.dubna 2014 .....

Poďakovanie: Touto cestou by som chcela vyjadriť vďaku všetkým, ktorí mi v akejkoľvek miere pomohli pri tvorbe tejto práce, predovšetkým však Ing. Filipovi Řezáčovi za jeho cenné rady, ochotnú pomoc pri riešení problémov, poskytnutie materiálov a odborné vedenie.

Abstrakt

Táto bakalárska práca je zameraná na bezpečnosť vo VoIP technológii. Na začiatku sú objasnené základné pojmy IP telefónie. Ďalej práca definuje pojem honeypot a popisuje nástroje pre realizáciu honeypotov v IP telefónii. Obsahom práce je aj testovanie vybraných honeypotov a analýza výsledkov testov. Záver je potom venovaný návrhu zapojenia vhodných honeypotov pre využitie v praxi.

Kľúčové slová

bezpečnosť, Brekeke SIP Server, Dionaea, Honeypot, Kippo, SIP, SSH, útoky, VoIP

Abstract

This bachelor thesis is focused on security in VoIP technology. At the beginning, basic concepts of IP telephony are explained. Thesis defines Honeypot concept and describes tools for implementing Honeypots in IP telephony. The work also includes a testing of selected Honeypots and analysis of test results. The conclusion is focused on the diagram of honeypot network for use in practice.

Keywords

attacks, Brekeke SIP Server, Dionaea, Honeypot, Kippo, security, SIP, SSH, VoIP

Zoznam použitých termínov a skratiek

Zoradené abecedne:

BSD - Berkeley Software Distribution. Licencia pre slobodný software.
DHCP - Dynamic Host Configuration Protocol. Súbor zásad, ktorý umožňuje zariadeniam vyžiadanie a získanie IP adresy od servera.
DNS - Domain Name System. Systém ukladajúci prístup k informáciám o názve stroja a domény.
DoS - Denial of Service. Druh útoku na zariadenie alebo službu v internetovej sieti.
GNU - Slobodný operačný systém typu Unix.
HTTP - Hypertext Transfer Protocol. Protokol pre prenos dokumentov medzi klientmi a servermi služby World Wide Web.
HTTPS - Hypertext Transfer Protocol Secure. Zabezpečený HTTP protokol.
ID - Identifikačné číslo.
IP - Internet Protocol. Základný komunikačný protokol internetu.
IPv4 - Internet Protocol version 4.Štvrtá verzia internetového protokolu.
IPv6 - Internet Protocol version 6. Štiesta verzia internetového protokolu.
NAT - Network Address Translation. Funkcia pre preklad sieťových adries.
OS - Operačný systém.
OSI - Open Systems Interconnection Reference Model. Model rozdeľujúci sieťové protokoly do vrstiev.
RTP - Real-time Transport Protocol. Protokol pre komunikáciu v reálnom čase.
SIP - Session Initiation Protocol. Signalizačný protokol pre multimediálne spojenie cez internet.
SMTP - Simple Mail Transfer Protocol. Protokol zaisťujúci prenos e-mailov.
SPIT - Spam over Internet Telephony. Spam v internetovej telefónii.
SSH - Secure Shell. Sieťový protokol pre zabezpečenú dátovú komunikáciu.
SW - Software.
TFTP - Trivial File Transfer Protocol. Jednoduchý protokol pre prenos súborov medzi počítačmi obsahujúci základné funkcie protokolu FTP.
TLS - Transport Layer Security. Protokol slúžiaci na šifrovanie dát.
UDP - User Datagram Protocol. Protokol pre prenos datagramov v sieti.
URI - Uniform Resource Identifier. Reťazec znakov používaný pre identifikáciu zdroja.
VoIP - Voice over Internet Protocol. Technológia pre prenos hlasu prostredníctvom internetového protokolu.

Obsah

Úvod

V dnešnej dobe čoraz viac veľkých spoločností využíva komunikáciu pomocou IP telefónie. S popularitou týchto technológií narastá aj potreba zabezpečenia nových služieb, ktorú spôsobuje zvýšený záujem útočníkov. Nezabezpečená IP telefónia je jednoducho odpočúvateľná, mnoho firiem sa tiež stretáva s nevyžiadanými telefonátmi alebo sociálnym inžinierstvom.

Pre ochranu infraštruktúry je potrebné držať krok s útočníkmi a neustále zlepšovať bezpečnostné opatrenia. Jedným zo spôsobov je sledovanie podozrivej aktivity pomocou honeypotov. Ich použitím získame údaje o aktivitách útočníkov a aktuálnych útokoch v sieti.

Táto bakalárska práca je v úvode venovaná základným pojmom a protokolom IP telefónie, ktoré čitateľ potrebuje poznať pre hlbšie pochopenie ďalšieho textu. Druhá kapitola sa zaoberá problematikou bezpečnostných rizík vo VoIP SIP telefónií a tiež popisom najvyužívanejších spôsobov útoku. Ďalšia časť je určená na zoznámenie sa s nástrojmi pre realizáciu honeypotov v internetovej telefónii, okrem riešení pre VoIP siete budú uvedené tiež SSH honeypoty súvisiace s nasadením SIP serverov. Nasledujúce kapitoly sú venované praktickej realizácii a implementácii vybraných honeypotov, ktoré sú pre nasadenie v reálnej prevádzke najvhodnejšie, analýze výsledkov a teoretickému návrhu využitia vhodného honeypotu v praxi.

Hlavným cieľom tejto práce je vytvorenie komplexnej analýzy dostupných honeypotov pre IP telefóniu a protokol SIP, ich praktické testovanie a návrh toho najvhodnejšieho pre využitie v praxi.

1 Základy IP telefónie

Táto kapitola je venovaná základným pojmom a protokolom IP telefónie, ktoré je potrebné poznať pre hlbšie pochopenie problematiky jej zabezpečenia.

1.1 VoIP

VoIP (Voice over Internet Protocol) je technológia, ktorá umožňuje prenos digitalizovaného hlasu a signalizácie cez internetový protokol. Využíva sa pre telefonovanie prostredníctvom internetu alebo iných packetovo prepínaných sietí. Táto technológia pre prenos dát štandardne používa protokoly UDP, RTP a pre signalizáciu a vyjednanie parametrov spojenia používa protokoly SIP [3].

1.2 UDP

UDP (User Datagram Protocol) [3] je jednoduchý protokol transportnej vrstvy OSI modelu. Jeho hlavnou úlohou je delenie dát do datagramov. UDP datagramy sú odosielané takou rýchlosťou, akú dovoľuje prenosové médium, bez záruky doručenia či dodania v správnom poradí.

Ďalšou úlohou UDP protokolu je multiplexovanie relácií. Sú známe tri druhy portov na štvrtej vrstve OSI modelu, ktoré sa za týmto účelom používajú:

- Dobre známe porty – pevne priradené porty stanovené pre protokoly vyšších vrstiev
- Zaregistrované porty – spoločnosťami registrované porty
- Dynamické porty – porty neviazané na konkrétny protokol

1.3 RTP

RTP (Real-time Transport Protocol) je nespojovo orientovaný transportný protokol. Slúži pre prenos audio či video dát v reálnom čase, zaisťuje zoradenie zaslaných packetov a ich časové značkovanie. Jeho ďalšou vlastnosťou je multiplexovanie a demultiplexovanie. Protokol RTP je vhodný pre vytváranie audio/video konferencií, keďže okrem prenášania dát medzi jedným odosielateľom a jedným príjemcom (Unicast) umožňuje tiež prenášanie dát medzi jedným odosielateľom a niekoľkými príjemcami (Multicast) [2].

1.4 SIP

SIP (Session Initiation Protocol) [1][3] je signalizačný protokol využívaný pre zostavenie, modifikáciu a ukončenie spojenia s jedným alebo viac účastníkmi. Je typu klient - server, pod pojmom klient si môžeme predstaviť IP telefón či SW aplikáciu a pojmom server je označený aplikačný server služieb. Komunikácia prebieha výmenou dvoch typov správ - žiadostí a odpovedí.

V jadre SIP protokolu je špecifikovaných niekoľko metód žiadostí, uvádzam najdôležitejšie:

INVITE je žiadosť o nadviazanie spojenia. Telo správy obsahuje jeho popis.

ACK potvrdzuje prijatie konečnej odpovede na žiadosť INVITE.

BYE je správa, ktorou klient oznamuje, že chce ukončiť nadviazané spojenie.

CANCEL je metóda využívaná pre zrušenie zostavovaného spojenia.

REGISTER je žiadosť o registráciu užívateľa.

OPTIONS je metóda pre zistenie vlastností SIP zariadenia.

Na každú žiadosť musí byť odpoveď, výnimkou je len metóda ACK. Kód odpovede je celé číslo z rozsahu 100 až 699 a značí jej typ. Definovaných je celkom 6 tried:

1xx sú dočasné informatívne odpovede

2xx sú pozitívne finálne odpovede

3xx sú odpovede využívané na presmerovanie

4xx sú negatívne konečné odpovede znamenajúce problém na strane klienta

5xx sú negatívne konečné odpovede a znamenajú problém na strane servera

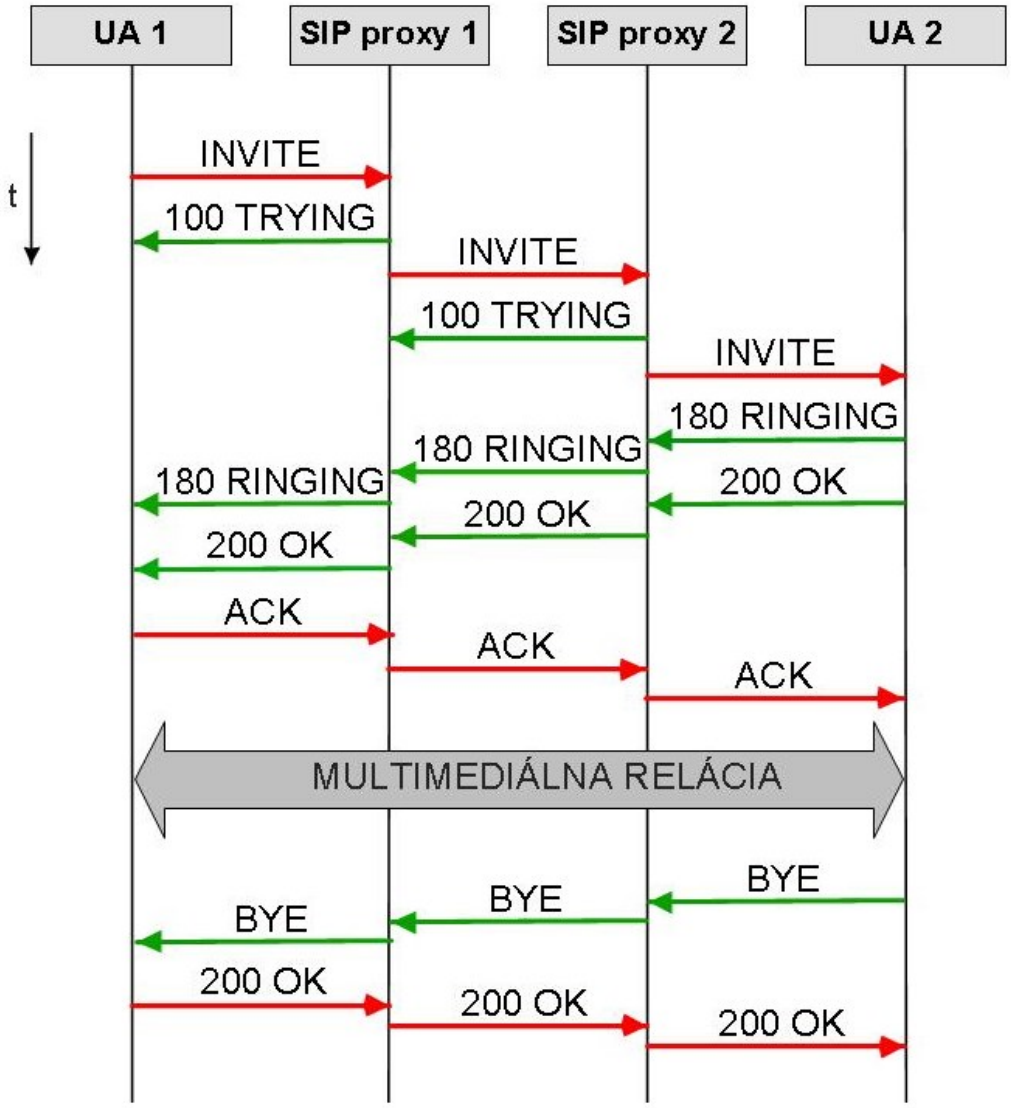
6xx predstavujú globálnu chybu

SIP je textovo orientovaný protokol podobný protokolom HTTP a SMTP. Klient posiela žiadosti na server, ktorý zasiela odpovede. V hlavičkách sa nachádzajú položky ako From, To, Subject. SIP entita je viazaná k doméne obsluhovanej SIP Proxy, medzidoménová komunikácia prebieha medzi rôznymi SIP Proxy. SIP entity sú identifikované použitím menných identifikátorov SIP URI (Uniform Resource Identifier), ktorých všeobecný tvar je nasledujúci:

sip:user:password@host:port;uri-parameters?headers

Základné prvky SIP siete:

- SIP user agent (UA) - koncové body, na ktorých vzniká SIP relácia. Obvykle sú predstavované koncovými terminálmi vo forme SW SIP telefónu či aplikáciami.
- SIP proxy, registrar, redirect a location server, v praxi implementované do jedného zariadenia nazývaného SIP server. Jeho úlohou je smerovanie žiadostí o spojenie, realizácia doplnkových služieb, autentizácia a pod.



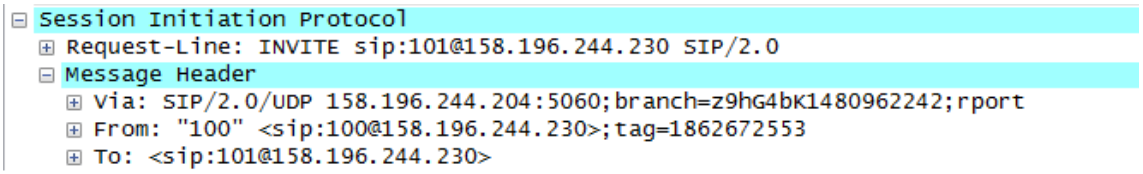
Obr. 1.1 Transakcia v SIP protokole

2 Bezpečnostné riziká vo VoIP SIP telefónii

Spôsobov, ako útočiť na VoIP sieť, je veľké množstvo a stále sa objavujú nové možnosti [24]. Infraštruktúra IP telefónie sa okrem telefónov a serverov skladá z rôznych podporných prvkov, ktorých aj malá zmena nastavenia stačí na zneužitie, či dokonca vyradenie siete z činnosti. V tejto kapitole sa zameriam na útoky na protokol SIP.

2.1 Mapovanie čísel

Využitím napr. aplikácie Wireshark [14] môže útočník pasívne monitorovať a zbierať všetky prichádzajúce a odchádzajúce hovory v danej sieti. V tomto prípade môže útočník vyfiltrovať protokol SIP a v žiadosti INVITE vyhľadať čísla a mená SIP účtov nachádzajúce sa v poliach "From" a "To". Vďaka týmto informáciám potom útočník môže vytvárať ďalšie útoky, ako sú nevyžiadané telefonáty a pod. [3].



Obr. 2.1 Žiadosť INVITE a polia "From" a "To"

2.2 Modifikácia a manipulácia signalizácie

Zmena signalizácie vo VoIP infraštruktúre môže spôsobiť veľké zmeny v nadviazanej relácii. Týmto zmenám hovoríme narušenie integrity hovoru. V nasledujúcich podkapitolách uvádzam príklady takýchto útokov.

2.2.1 Odobranie registrácie

Žiadosťou REGISTER sa na SIP server po zapnutí registruje každé koncové zariadenie a túto žiadosť následne opakovane posiela, väčšinou v intervale 3600 sekúnd. Vďaka registrácii SIP server vie, kam má smerovať prichádzajúce hovory. Ak však registráciu odstránime, koncové zariadenie nebude schopné hovory prijímať. Tento útok je jednoduchý, no veľmi účinný [3].

2.2.2 Pridanie registrácie

Rovnako, ako sme schopní registráciu odobrať, je tiež možné ju priradiť. VoIP infraštruktúra založená na SIP protokole umožňuje priradenie viac kontaktov na jednu registráciu. V praxi to znamená, že v prípade prichádzajúceho hovoru môže súčasne vyzváňať viac telefónov v rôznych lokalitách. Útočník tak napríklad po pridaní registrácie na vlastné koncové zariadenie môže jednoducho hovor prijať ako prvý [3].

2.3 Skenovanie a monitorovanie siete

Monitorovanie siete nie je priamo zamerané na VoIP služby. Infraštruktúra internetovej telefónie sa okrem VoIP serverov a telefónov skladá aj z rôznych podporných prvkov, ako sú napríklad DHCP server, TFTP server, DNS server. Útočník tieto prvky lokalizuje a získava o nich užitočné informácie. Skenovaním siete je možné získavať zoznamy účtov zo servera, ktoré môžu byť využité pri ďalších útokoch [3].

2.4 DoS útoky

DoS (Denial od Service) sú útoky, ktoré rôznymi formami zabraňujú užívateľom využívať potrebné služby, prípadne ich funkčnosť obmedzia natoľko, že sú takmer nepoužiteľné [23]. V prípade VoIP môže aj menší útok spôsobiť nepoužiteľnosť služieb. V internetovej telefónii sa DoS útoky zameriavajú hlavne na signalizačné a transportné protokoly.

Útok DoS na signalizačný protokol, akým je SIP, býva veľký problém, pretože môže byť napadnutá ktorákoľvek časť VoIP siete. Najčastejším cieľom býva SIP proxy server. Príkladom je záplavový (flood) útok, pomocou ktorého sa vygeneruje také množstvo žiadostí, že vyťažia server, a nie je možné nadviazať hovor.

Záplavový útok je efektívny aj na transportné protokoly. Patrí medzi ne RTP protokol, ktorý prenáša dáta v reálnom čase a vo VoIP sieťach je využívaný prakticky najviac. Cieľom bývajú koncové IP telefóny, ktoré sú po útoku takmer alebo úplne nepoužiteľné [3].

2.5 SPIT

SPIT (Spam over Internet Telephony) [3] síce nie je útok na protokol SIP, napriek tomu by som ho rada spomenula, keďže sa stáva čoraz rozšírenejším. Radí sa medzi tzv. sociálne hrozby, a podobne ako SPAM v e-mailovej pošte, je určený na obťažovanie užívateľa reklamnými či inými hovormi. V súčasnosti už pre generovanie SPITu existujú nástroje, ako napríklad aplikácia Spitter pobočkovej ústredne Asterisk. Na rozdiel od e-mailového SPAMu je detekcia SPITu zložitejšia, pretože je nutné mu zabrániť v reálnom čase a jeho údaje sú veľmi podobné tým, ktoré má bežný hovor.

3 Nástroje pre realizáciu honeypotov v IP telefónii

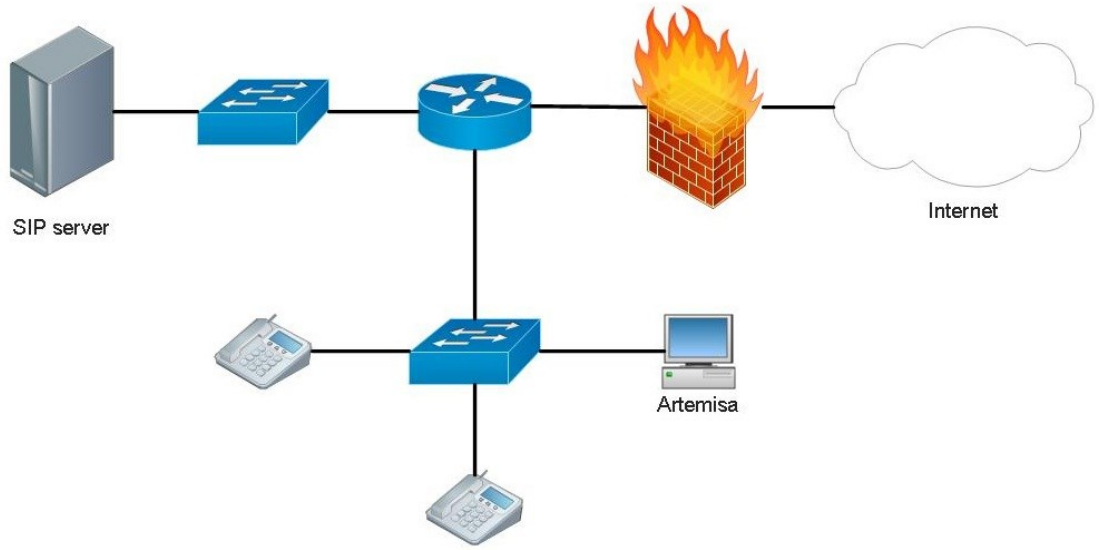
Pod pojmom honeypot sa skrýva služba zámerne vystavená riziku útoku. Honeypoty sú navrhnuté na odhalenie nedostatočného zabezpečenia a získavanie informácií o priebehu útoku. Tie bývajú využívané na odhaľovanie nových metód útokov a pri prevencii incidentov. Účelom honeypotov môže byť aj to, že sú vystavované útokom namiesto významných systémových zdrojov.

Pôsobia ako reálny systém a na základe toho aj rovnako komunikujú s okolím. V súčasnej dobe existuje mnoho honeypot riešení napodobňujúcich rôzne služby. V nasledujúcich podkapitolách uvediem niekoľko riešení pre VoIP siete a takisto SSH honeypoty, ktoré súvisia s nasadením SIP serverov.

3.1 Artemisa

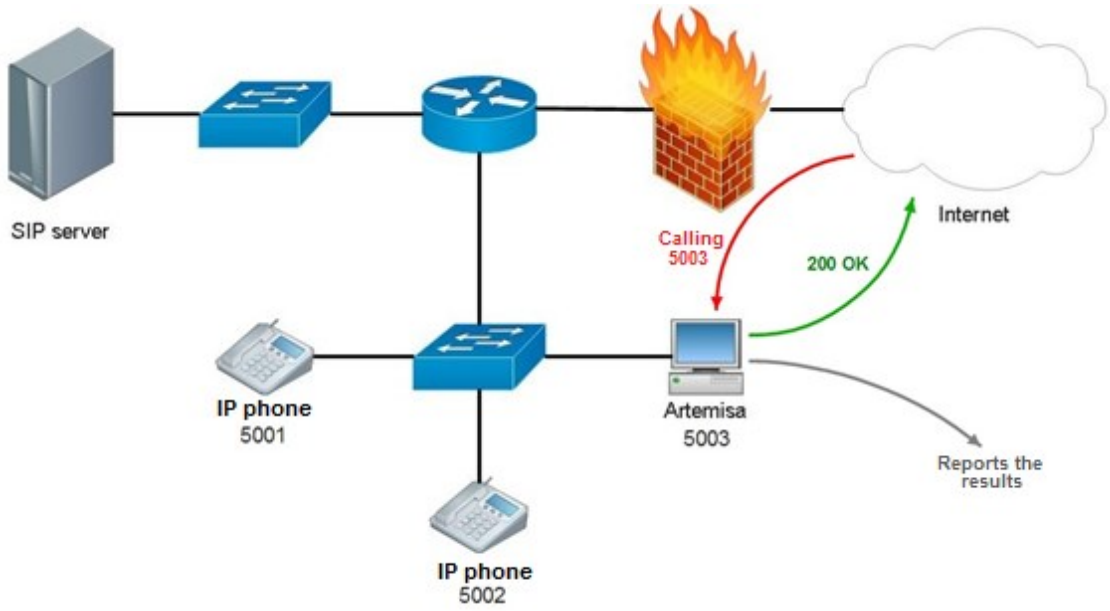
Artemisa [4] je honeypot nasadzovaný vo VoIP sieti na protokole SIP, ktorý umožňuje odhaliť škodlivé aktivity v ranom štádiu. Simuluje koncový bod a čaká na prichádzajúce útoky. Pri nadviazaní relácie odpovedá na prichádzajúce hovory a následne skúma SIP správy. Kontroluje doménové mená, SIP porty a odtlačky známych hackovacích nástrojov, vďaka čomu je schopný zistiť prítomnosť nepriateľskej aktivity. Takisto kontroluje prijatý RTP tok. Audio stopu spolu s ostatnými výsledkami nakoniec ukladá do vopred definovanej zložky, prípadne získané informácie odošle do e-mailovej schránky.

Artemisa takisto môže byť využívaná pre real-time nastavovanie firewallu-zakazovanie IP adries, alebo v prípade pobočkových ústrední zakazovanie ID volajúceho.



Obr. 3.1 VoIP topológia s honeypotom Artemisa

Nasledujúci obrázok popisuje, ako Artemisa pracuje: honeypot tváriaci sa ako SW telefón obdrží žiadosť o nadviazanie relácie, na ktorú odpovie a zároveň zaznamenáva jej priebeh. Po ukončení hovoru odosiela jeho vyhodnotenie na preddefinovanú e-mailovú adresu.



Obr. 3.2Artemisa - nadviazanie relácie

3.2 Dionaea

Dionaea [6][18] patrí k honeypotom, ktoré dokážu simulovať viac služieb naraz. Okrem SIP protokolu sú to napríklad HTTP a HTTPS, FTP, Microsoft SQL server. Podporuje operačný systém Linux, IPv4 aj v IPv6 a zabezpečovací protokol TLS. V prípade simulácie protokolu SIP Dionaea pracuje iným spôsobom ako Artemisa. Nie je potrebné pripájať sa na externý SIP server, namiesto toho len vyčkáva na prichádzajúce SIP správy a reaguje vytvorením relácie. Podporuje najčastejšie využívané žiadosti: INVITE, OPTIONS, ACK, BYE, CANCEL, rovnako ako aj multiplesession a RTP tok, ktorého audio stopa môže byť zaznamenaná. Celú komunikáciu monitoruje a následne ju ukladá do textového súboru, prípadne do SQLite databázy, vďaka čomu je aj možné jednoducho vytvárať štatistické grafy.

Pri svojej práci využíva nástroj P0f, ktorý sleduje odtlačky hackovacích nástrojov. Dokáže identifikovať systémy, ktoré sa k nemu pripájajú, ich vzdialenosť, prítomnosť firewallu, masquerading (prepis východiskovej adresy), spôsob pripojenia útočníka do siete a iné [8].

3.3 Kojoney

Produkt Kojoney je nízkointeraktívny honeypot napísaný v jazyku Python, licencovaný ako copyleft GNU General Public License, ktorý nie je priamo orientovaný na VoIP technológiu, simuluje SSH server. Po tom, ako sa útočník prihlási do siete s Kojoney, je presmerovaný do honeypotu, takže so skutočným systémom nemá možnosť komunikovať. Kojoney môže byť nakonfigurovaný s ľubovoľným počtom účtov a hesiel, umožňujúcich úspešnú autentifikáciu. Zaznamenáva všetky pokusy o pripojenie vrátane tých neúspešných, sleduje útočníkovu IP adresu a jeho pohyb v sieti. Útočník prihlásený v sieti s honeypotom môže zadávať len obmedzené množstvo príkazov, na ktoré bude Kojoney odpovedať už preddefinovaným textom.

Pre získavanie prehľadných informácií o prevádzke môže užívateľ využiť skript Kojreport, ktorý generuje textové správy z log súboru honeypotu. Tieto správy obsahujú informácie o úspešných a neúspešných pripojeniach na Kojoney, príkazy zadané počas pripojenia, IP adresy a krajiny, z ktorých sa útočník pripájal a iné.

3.4 Kippo

Kippo [17] je honeypot inšpirovaný produktom Kojoney, pod licenciou BSD, ktorá umožňuje voľné šírenie softwaru a vlastné úpravy skriptu. Kippo je vyvinutý na simuláciu SSH serveru. Ten býva častým cieľom útočníkov. Užívatelia pokúšajúci sa pripojiť na server, na ktorom beží aj Kippo, sú presmerovaní priamo do honeypotu. Táto situácia nastane v prípade, keď užívateľova IP adresa nie je v zozname povolených. Útočník je po prepojení do honeypotu vyzvaný na zadanie prihlasovacích údajov, ktoré sú nastavené na štatisticky najčastejšie používané užívateľské mená a heslá. Po zadaní platnej kombinácie je útočníkovi umožnený prístup k falošným súborom. Každý jeho krok je zaznamenaný do databázy, ktorej dáta potom slúžia na následnú analýzu [6].

Pre vizualizáciu štatistík z honeypotu Kippo bol vytvorený skript Kippo-Graph [15]. Ten zobrazuje 24 grafov, ako napríklad top 10 hesiel, top 10 užívateľských mien, pokusy o pripojenie za 1 deň a za 1 týždeň, IP adresy a krajiny pripojených, top 10 úspešných a neúspešných prístupov, pomer úspešnosti a mnoho iných.

3.5 Brekeke

Brekeke Software, Inc. je firma vyvíjajúca produkty zamerané na SIP protokol. Jedným z produktov je software Brekeke SIP Server určený pre operačné systémy Windows a Linux. Umožňuje vysoko kvalitnú a spoľahlivú komunikáciu cez internetový protokol. Jeho 60 dňová trial verzia je na oficiálnych stránkach spoločnosti poskytovaná na stiahnutie zdarma. Brekeke SIP Server je tvorený SIP Proxy serverom a Registrar serverom. Overuje a registruje VoIP zariadenia a smeruje SIP relácie. Pre zabránenie škodlivej činnosti, akou je SPIT alebo DoS, sa dá Brekeke SIP server nastaviť ako honeypot, napríklad zablokovaním SIP packetov, ak prenos nie je zabezpečený protokolom TLS (Transport Layer Security), blokovaním žiadostí z IP adries, ktoré sú mimo určený rozsah a pod.[10].

Brekeke SIP server poskytuje možnosť nastavenia času-koľko sekúnd má server čakať na odpoveď na žiadosť o nadviazanie relácie a vďaka funkcii NAT Traversal môžu byť k serveru pripojení klienti z rôznych sietí. Tento produkt tiež umožňuje na jednom serveri hostiť viac domén, pričom trial verzia je limitovaná na 2 domény a rozšírená edícia limitovaná nie je.

Rozšírená edícia poskytuje funkciu Heartbeat, ktorá slúži na prevzatie služieb pri zlyhaní. Sleduje vopred určené subjekty v sieti, ako napríklad iné Brekeke SIP Servery, a pri ich výpadku spustí preddefinované akcie (napr. prepínanie IP adries alebo upozornenie e-mailom). Je takto možné sledovať viac subjektov v sieti naraz. Brekeke SIP Server tiež obsahuje tzv. Dial Plan definujúci rôzne pravidlá. Administrátor tak môže upravovať hlavičku SIP protokolu, smerovanie, filtrovanie, nastavenia RTP spojení a iné.

4 Nasadenie honeypotov v SIP infraštruktúre

Táto kapitola je venovaná praktickej realizácii a implementácii vybraných honeypotov. Pre hlbšiu analýzu vlastností a využiteľnosti v IP telefónii bude použitý honeypot Dionaea, bude otestovaný software Brekeke SIP Server a pre sledovanie ostatných služieb bude použitý honeypot Kippo. Tieto produkty sú z pohľadu využívanosti, dostupnej podpory a aktuálnosti najvhodnejšie pre nasadenie v reálnej prevádzke.

4.1 BackTrack

BackTrack [12] je Linuxová distribúcia špecializovaná na prienikové testy operačných systémov a počítačových sietí, ktorú som využívala pri testovaní vybraných honeypotov. Obsahuje skripty pre penetračné testy, je vydávaný ako LiveCD alebo LiveUSB v grafickom alebo textovom rozhraní. Zahŕňa aplikácie ako Wireshark alebo Nmap. Nástroje na testovanie rozdeľuje do dvanástich kategórií zobrazených na obrázku 4.1, medzi ktoré patria Zisťovanie hesiel, Skenery, Maskovanie, Odchytávanie packetov, Cisco nástroje, Databázové nástroje a iné. Vďaka BackTracku má užívateľ k dispozícii veľké množstvo nástrojov pre testovanie a útoky na VoIP technológiu. Medzi najzaujímavejšie nástroje patria SMAP, ktorý zasielaním SIP žiadostí skenuje VoIP zariadenia v sieti, VoIPong detekujúci hovory vrátane tých, ktoré sú kódované, IAXflood určený pre zahltenie cieľa IAX2 protokolmi, ktoré využíva pobočková ustredňa Asterisk, alebo Teardown, ktorý zasielaním BYE žiadostí ukončuje SIP relácie. Distribúcia BackTrack už nie je naďalej udržovaná, nahradil ju projekt Kali, ktorý z BackTracku priamo vychádza. Vzhľadom k jeho stálemu vývoju nie je zatiaľ táto verzia stabilná, preto som sa pri svojej práci rozhodla využívať poslednú verziu BackTracku.

Obr. 4.1 BackTrack - grafické rozhranie

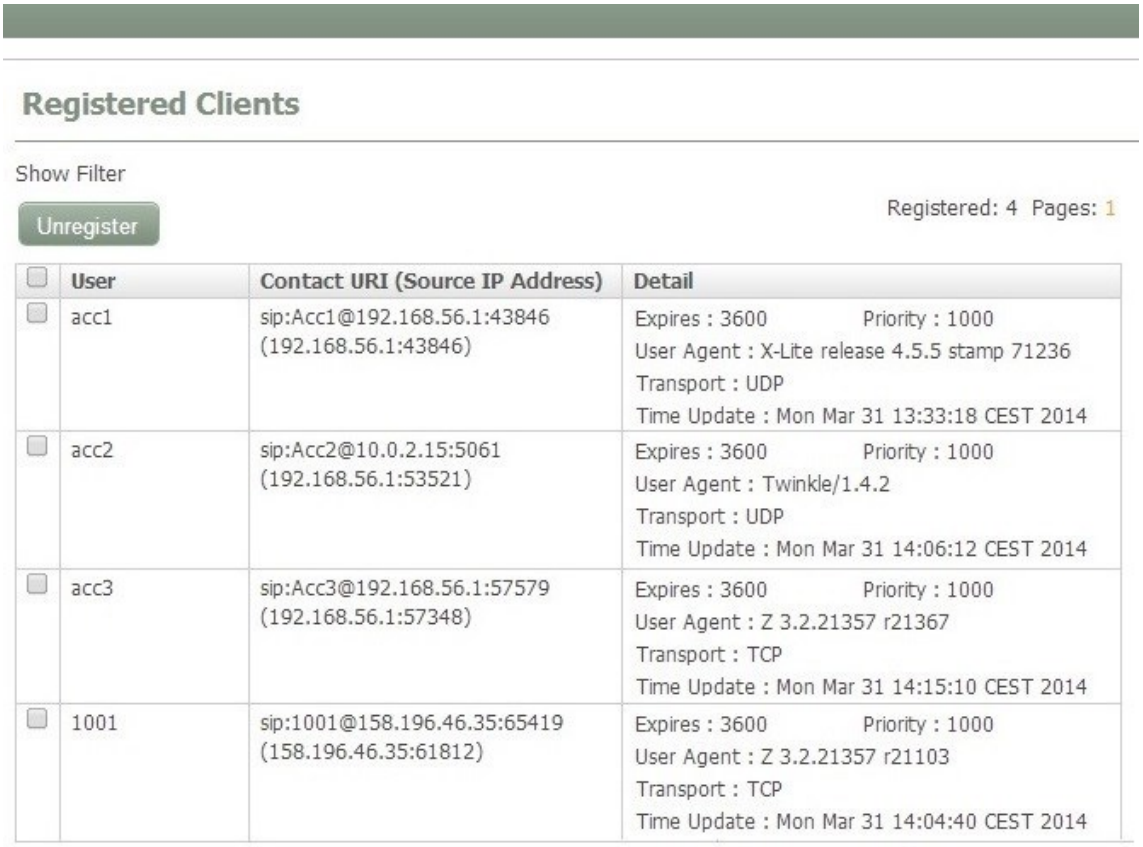
4.2 VirtualBox

VirtualBox [11] je virtualizačný nástroj firmy Oracle, ktorý som využívala pri testovaní vybraných honeypotov. Podporuje OS Windows, Linux, Mac OS X a Solaris, ktoré tak môžu hosťovať veľké množstvo operačných systémov. Na jednom počítači umožňuje spúšťať viac OS naraz, jediným obmedzením užívateľa je voľné miesto na disku a v pamäti. Je možné zdielať súbory medzi hosťujúcim a virtuálnym systémom. Medzi základné funkcie nástroja VirtualBox patria: snímky – pomocou tzv. Snapshots je možné uložiť určitý stav virtuálneho počítača pre neskoršie použitie, pričom ich počet nie je limitovaný; možnosť ovládania produktu cez príkazový riadok; podpora hardwarovej virtualizácie spoločností AMD a Intel.

4.3 Inštalácia a konfigurácia Brekeke SIP Servera

Ako prvú som z oficiálnych stránok získala voľne dostupnú 60-dňovú trial verziu Brekeke SIP Servera. Po nainštalovaní a zadaní dočasnej licencie som sa pomocou prístupovej obrazovky a pridelených údajov prihlásila do konfiguračného rozhrania. Na obrázku 4.2 je zobrazený stav servera po spustení.

Obr. 4.2 Brekeke SIP Server - Status

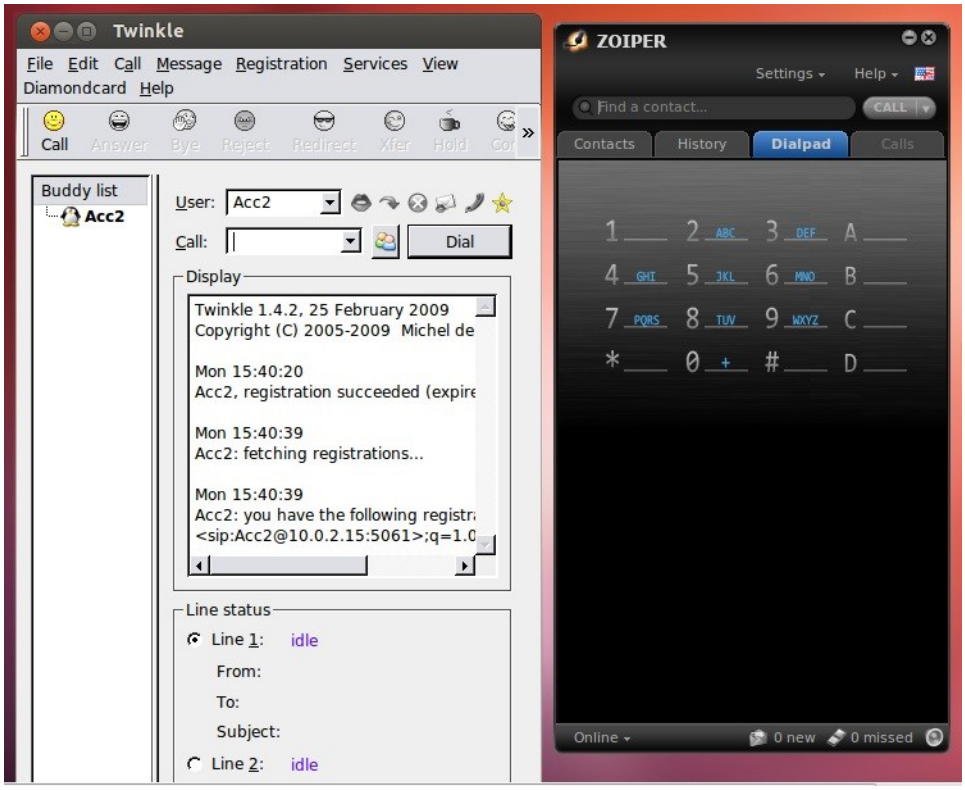


Obr. 4.3 Brekeke SIP Server - Registrovaní klienti

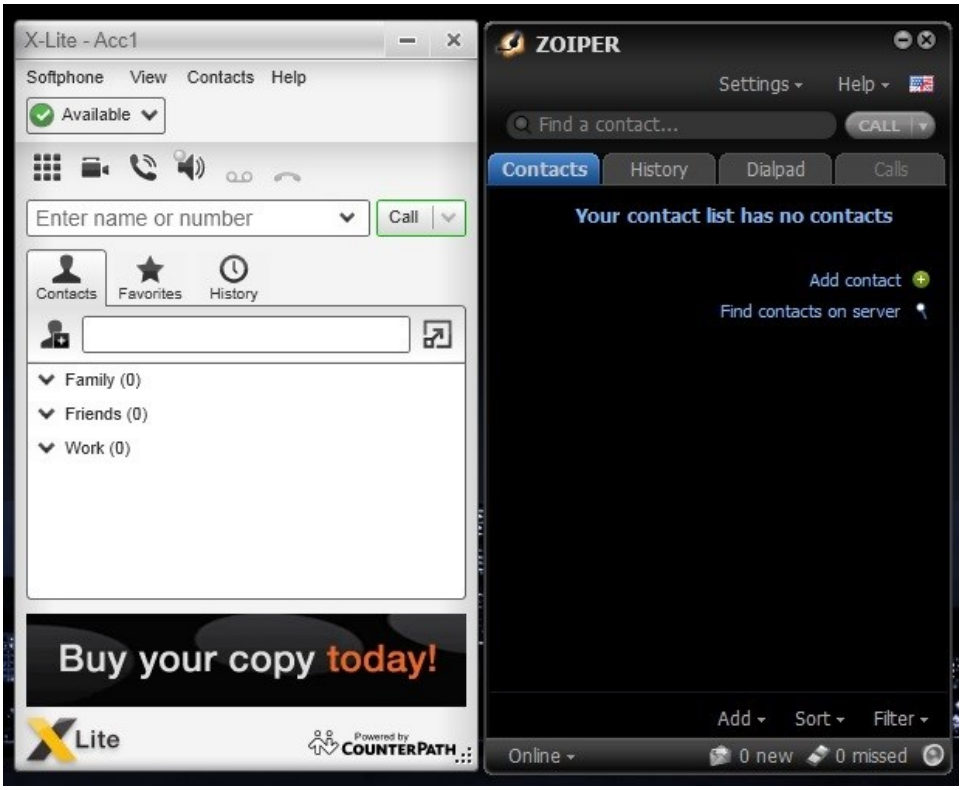
Na obrázku 4.3 je zobrazený zoznam registrovaných klientov. Ako koncové zariadenia som využila softwarové telefóny nainštalované v operačnom systéme Windows a v Linuxovej distribúcii Ubuntu spúšťanej vo virtuálnom počítači.

V OS Windows boli použité produkty X-Lite a Zoiper, v Linuxovej distribúcii produkty Twinkle a Zopier. Tieto koncové zariadenia sú zobrazené na obrázkoch 4.4 a 4.5.

- X-Lite je softwarový telefón spoločnosti Counter Path distribuovaný pod freeware licenciou. Tento nástroj poskytuje telefonovanie pomocou protokolu SIP a je dostupný pre OS Winsows a Mac OS X.
- Twinkle je softwarový telefón pre internetovú telefóniu pomocou protokolu SIP, poskytovaný len pre Linuxové distribúcie.
- Zoiper je VoIP softwarový telefón určený pre operačné systémy Windows, Linux, Mac OS X, pre platformy Android, iOS a Windows Phone, a takisto aj pre rôzne webové prehliadače. Je dostupný vo verzii Free obsahujúcej základné funkcie a v spoplatnenej verzii Business.



Obr. 4.4 Produkty použité v OS Linux



Obr. 4.5 Produkty použité v OS Windows

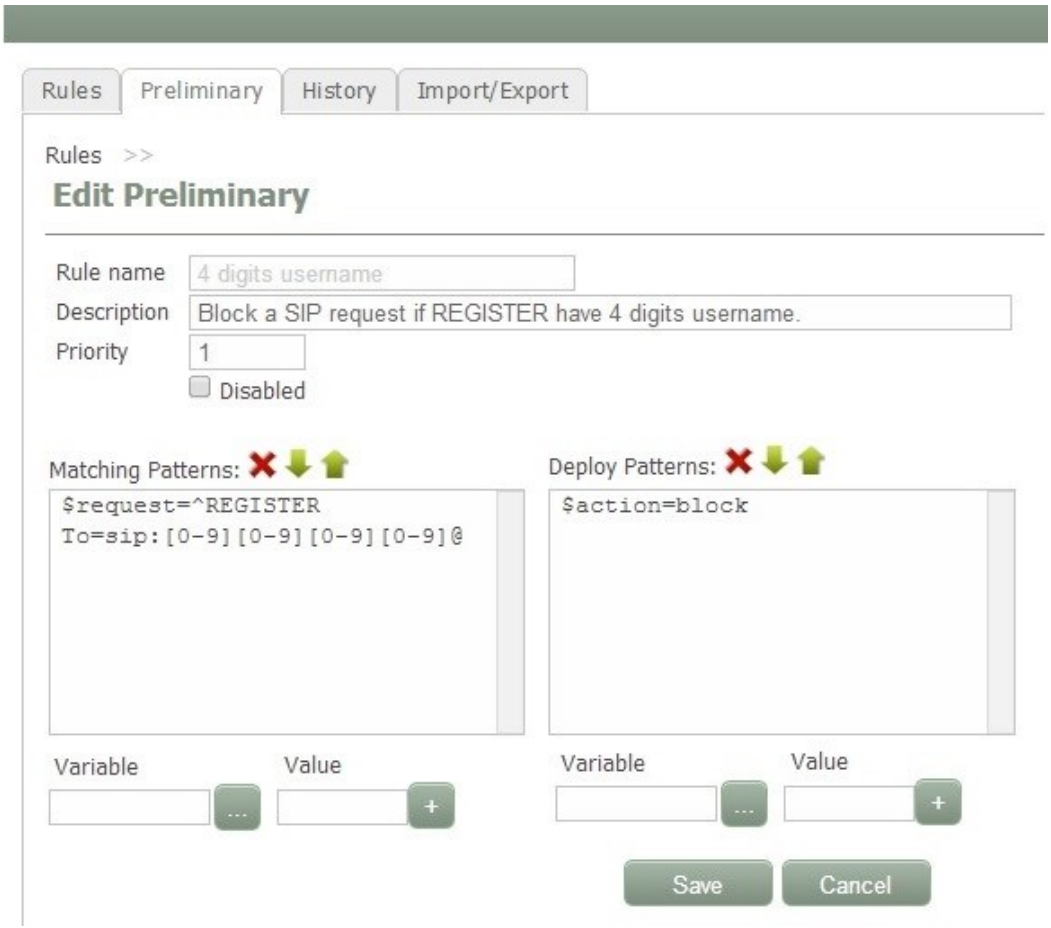
4.4 Testovanie Brekeke SIP Servera

4.4.1 Blokovanie užívateľov

Produkt Brekeke SIP Server samotný neposkytuje služby honeypotu, avšak pri správnom nastavení je možné simulovať niektoré jeho vlastnosti. Je tak možné napríklad zablokovať užívateľov volajúcich z IP adries, ktoré nespadajú do povoleného rozsahu, alebo užívateľov, ktorí majú globálnu IP adresu [10].

Pre otestovanie týchto vlastností Brekeke SIP Servera som zvolila situáciu, kedy bude zablokovaný každý volajúci s telefónnym číslom, ktoré je zložené práve zo štyroch čísel. Ako je vidieť na obrázku 4.6, bolo to docielené zadaním príkazov

```
[MatchingPatterns] $request=^REGISTER To=sip:[0-9][0-9][0-9][0-9]@
[DeployPatterns] $action=block
```



Obr. 4.6 Brekeke SIP Server – blokovanie SIP žiadostí

4.4.2 **DoS útoky**

Pre testovanie odolnosti Brekeke SIP Servera voči DoS útoku som zvolila nástroj Inviteflood systému BackTrack, ktorý sa nachádza v kategórii "StressTesting" a nástroj UDPflood [13], ktorý bol do BackTracku doinštalovaný.

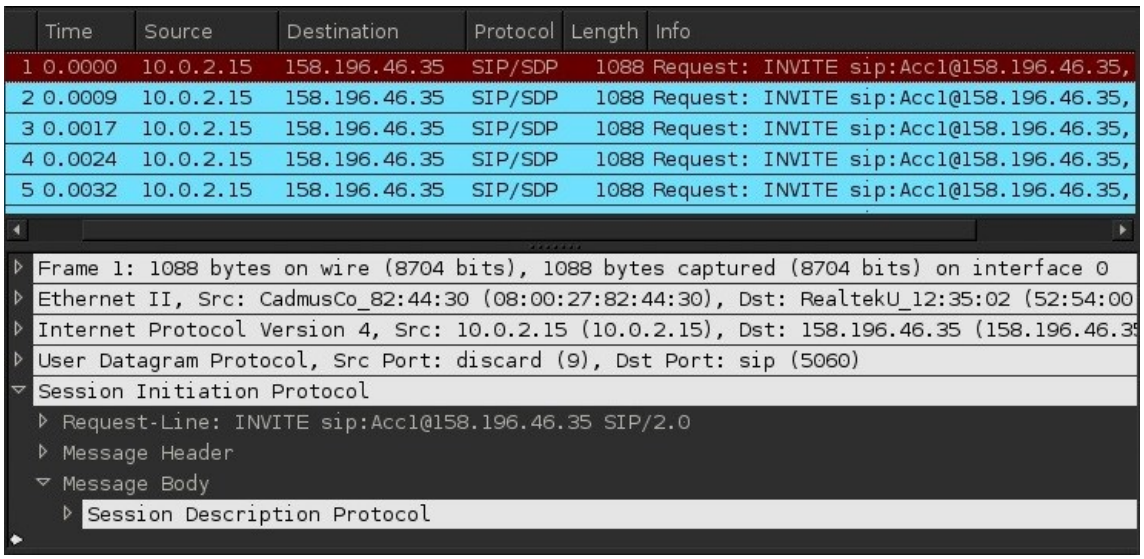
Nástroj Inviteflood je určený na zahltenie cieľového IP telefónu SIP INVITE žiadosťami. Po zadaní príkazu v tvare

```
./inviteflood eth0 názov_cieľového_účtu cieľová_doména IP_adresa_cieľa počet_zaslaných_žiadostí
```

bolo na koncové zariadenie zaslaných 10 000 000 INVITE žiadostí. Priebeh útoku zaznamenaný programom Wireshark[14] zobrazuje obrázok 4.7.

Nástroj UDPflood slúži na zahltenie cieľa packetmi UDP protokolu. Na koncové zariadenie bolo zaslaných 100 000 UDP packetov zadaním príkazu v tvare

```
./udpflood meno_zdroja meno_cieľa port_zdroja port_cieľa počet_packetov
```



Obr. 4.7 Útok Inviteflood zaznamenaný programom Wireshark

4.5 Testovanie honeypotuDionaea

4.5.1 DoS útok

Pre testovanie honeypotu Dionaea voči DoS útokom som zvolila nástroj UDPflood, ktorý už bol spomínaný v predchádzajúcej podkapitole (4.4.2 DoS útoky). Ako je vidieť na obrázku 4.8, na IP adresu, na ktorej je spustená Dionaea, bolo odoslaných 100 000 UDP packetov.

```
root@bt:~/Desktop/udpflood# ./udpflood 192.168.56.102 192.168.56.101 5060 5060 100000
Will flood port 5060 from port 5060 100000 times
We have IP_HDRINCL

Number of Packets sent:

Sent 100000
root@bt:~/Desktop/udpflood#
```

Obr. 4.8 Útok UDPflood

4.5.2 Nástroje SIPVicious

SIPVicious je sada nástrojov, ktoré sú navrhnuté pre testovanie vo VoIP SIP telefónii. Z nich som na testovanie honeypotu Dionaea vybrala SVmap a SVwar.

SVmap je nástroj na skenovanie a identifikáciu zariadení na jednej či viacerých IP adresách. Po zadaní príkazu v tvare `./svmap.py cieľová_IP_adresa` sa zobrazí zoznam dostupných zariadení.

SVwar slúži pri skúmaní VoIP služieb a zariadení na zvolenej IP adrese. Funguje na princípe skúmania získaných odpovedí na odoslané žiadosti. Ja som pri testovaní využila postupne metódy OPTIONS, INVITE a REGISTER.

4.5.3 Metasploit

Metasploit je sada nástrojov navrhnutých na prienikové testovanie a získavanie informácií o nedostatočnom zabezpečení, obsahujúca tiež nástroje určené pre VoIP sieť. Spomedzi nich som na testovanie honeypotu Dionaea vybrala modul Metasploit Enumerator, ktorý môže byť útočníkmi zneužívaný na objavovanie platných SIP účtov pomocou metódy REGISTER alebo OPTIONS. Po vstupe do msf konzoly (pomocou príkazu `msfconsole`) a zadaní príkazu `usescanner/sip/enumerator` som nastavila požadovanú cieľovú IP adresu (`set RHOSTS IP_adresa`) a spustila útok pomocou príkazu `run`.

4.6 Testovanie honeypotuKippo

4.6.1 Nástroj Hping3

Hping3 je nástroj navrhnutý na testovanie bezpečnosti siete. Funguje formou odosielania napr. UDP alebo TCP packetov a pracuje podobne ako klasický ping. Ako je vidieť na obrázku 4.9, zadaním príkazu v tvare

`hping3 parametre cieľová_IP_adresa -p číslo_portu -c počet_packetov`

bol na IP adresu, na ktorej je spustené Kippo a SSH port 22, odoslaný požadovaný počet packetov.

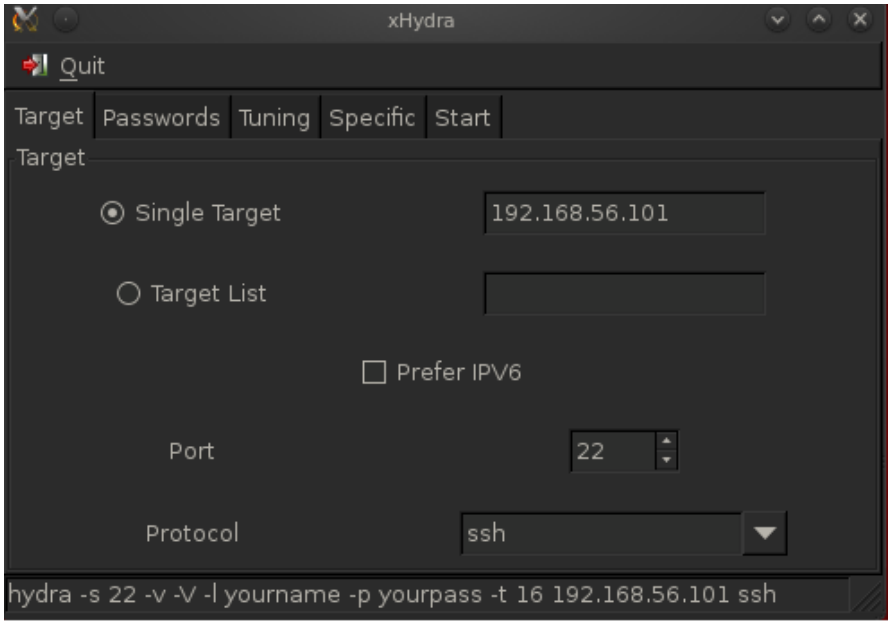
```
root@bt:~# hping3 -S 192.168.56.101 -p 22 -c 4
HPING 192.168.56.101 (eth0 192.168.56.101): S set, 40 headers + 0 data bytes
len=46 ip=192.168.56.101 ttl=64 id=6637 sport=22 flags=SA seq=0 win=65535 rtt=4.5 ms
len=46 ip=192.168.56.101 ttl=64 id=6638 sport=22 flags=SA seq=1 win=65535 rtt=2.0 ms
len=46 ip=192.168.56.101 ttl=64 id=6639 sport=22 flags=SA seq=2 win=65535 rtt=2.7 ms
len=46 ip=192.168.56.101 ttl=64 id=6640 sport=22 flags=SA seq=3 win=65535 rtt=3.3 ms

--- 192.168.56.101 hping statistic ---
4 packets tramitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.0/3.1/4.5 ms
root@bt:~#
```

Obr. 4.9 Nástroj Hping3

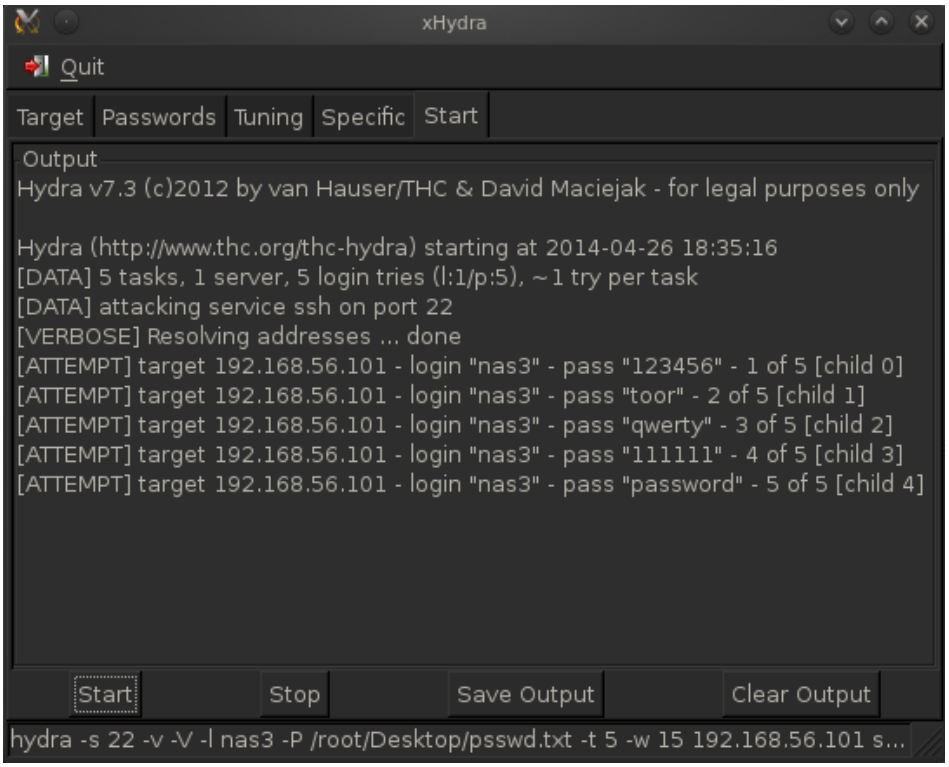
4.6.2 XHydra

XHydra je nástroj systému BackTrack na prelomenie užívateľských mien a hesiel pomocou slovníkového útoku. Ako je vidieť na obrázku 4.10, je možné ho spustiť v grafickom režime. Útočník má možnosť zvoliť testovanie jednej alebo viacerých cieľových IP adries.



Obr. 4.10 Nástroj XHydra – grafické prostredie

Po zadaní cieľovej adresy je potrebné zadať cieľový port a následne zvoliť cestu k zoznamom užívateľských mien a hesiel, ktoré budú využité pri testovaní. Obrázok 4.11 zachytáva nástroj XHydra počas útoku.



Obr. 4.11 Nástroj XHydra počas útoku

4.6.3 **Ncrack**

Ncrack je nástroj určený na prelomenie hesiel. Podporuje Linuxové platformy, OS Windows, MAX OS X a tiež veľké množstvo protokolov, vrátane protokolu SSH, ktorý bol využívaný pri testovaní. Po zadaní príkazu v tvare

`ncrack –p číslo_portu –usermeno_cieľa –P zoznam_hesiel cieľová_adresa`

sa nástroj sa pokúša o prelomenie hesla. Pri tomto útoku som využila zoznam štatisticky najpoužívanejších hesiel, medzi ktoré patrilo aj heslo pre honeypot Kippo.

5 Analýza výsledkov a návrh využitia vhodného honeypotu v praxi

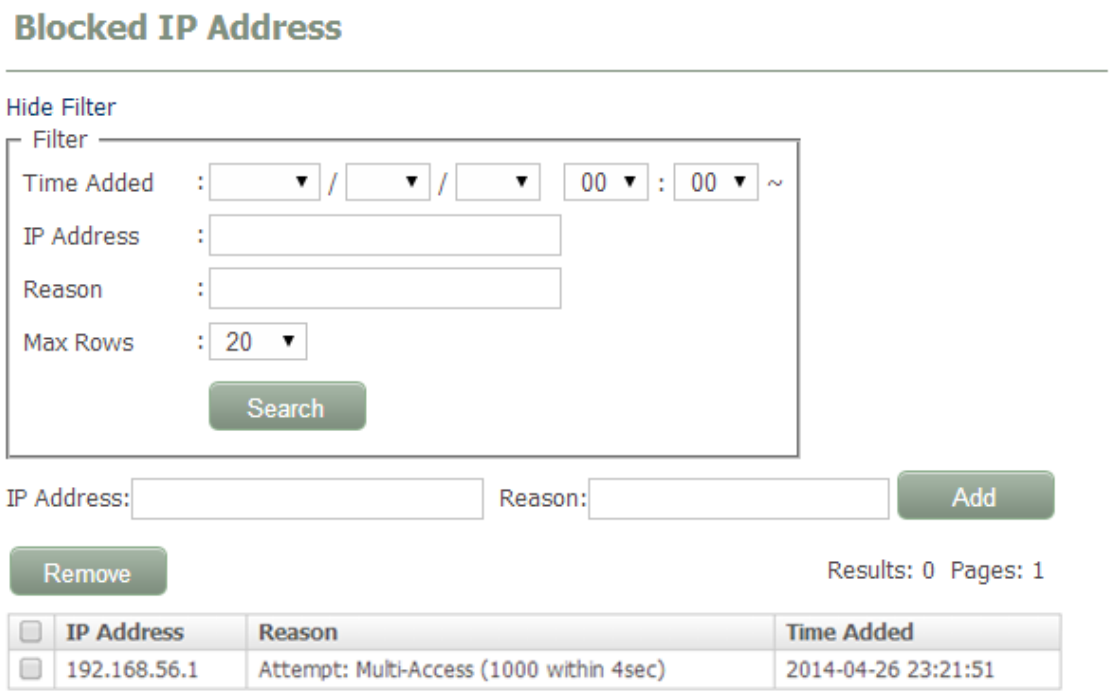
5.1 Výsledky testovania Brekeke SIP Servera

5.1.1 Blokovanie užívateľov

Pred aplikovaním pravidla, ktoré blokuje každého volajúceho s telefónnym číslom zloženým práve zo štyroch čísel, mohli medzi sebou zaregistrovaní užívatelia Acc1, Acc2, Acc3 a 1001 nadväzovať relácie, avšak po zadaní príkazov zobrazených na obrázku 4.6 nebolo koncové zariadenie 1001 schopné nadviazať spojenie so žiadnym zo spomínaných užívateľov.

5.1.2 DoS útoky

Počas útokov Inviteflood a UDPflood bolo koncové zariadenie schopné prijímať aj vytvárať hovory, avšak v niekoľkých prípadoch bolo nadviazané spojenie náhle prerušené. Ako je možné vidieť na obrázku 5.1, Brekeke SIP Server po ukončení útokov automaticky zaradil útočníkovu IP adresu do Block listu, takže následne sa nebolo možné z tejto IP adresy dovolať na žiaden zo zaregistrovaných účtov.



Obr. 5.1 Brekeke SIP Server - Blokovaná IP adresa

5.2 Výsledky testovania honeypotu Dionaea

5.2.1 DoS útok

Po zadaní potrebného príkazu a spustení útoku bolo na honeypot Dionaea úspešne odoslaných 100 000 UDP packetov. Funkčnosť honeypotu nebola obmedzená, Dionaea celú komunikáciu zaznamenávala. Časť zo zachyteného útoku je možné vidieť na obrázku 5.2.

```
[27042014 11:08:37] connection connection.c:4337: connection 0x948d1e0 accept/ud
p/close [192.168.56.101:5060->192.168.56.1:59495] state: close->close
[27042014 11:08:37] sip dionaea/sip/__init__.py:564: SIP Session created with pe
rsonality 'default'
[27042014 11:08:37] connection connection.c:4337: connection 0x948df08 accept/ud
p/established [192.168.56.101:5060->192.168.56.1:59495] state: established->esta
blished
[27042014 11:08:37] logsql dionaea/logsql.py:618: connect connection to 192.168.
56.1/:59495 from 192.168.56.101:5060 (id=882)
[27042014 11:08:37] sip dionaea/sip/rfc3261.py:584: Can't parse first line of si
p message: b'1234567890\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
[27042014 11:08:37] connection connection.c:4337: connection 0x948df08 accept/ud
p/established [192.168.56.101:5060->192.168.56.1:59495] state: established->clos
e
[27042014 11:08:37] connection connection.c:4337: connection 0x948df08 accept/ud
p/close [192.168.56.101:5060->192.168.56.1:59495] state: close->close
[27042014 11:08:40] logsql dionaea/logsql.py:689: attackid 799 is done
[27042014 11:08:40] logsql dionaea/logsql.py:689: attackid 803 is done
```

Obr. 5.2 DoS útok zachytený honeypotom Dionea

5.2.2 Nástroje SIPVicious

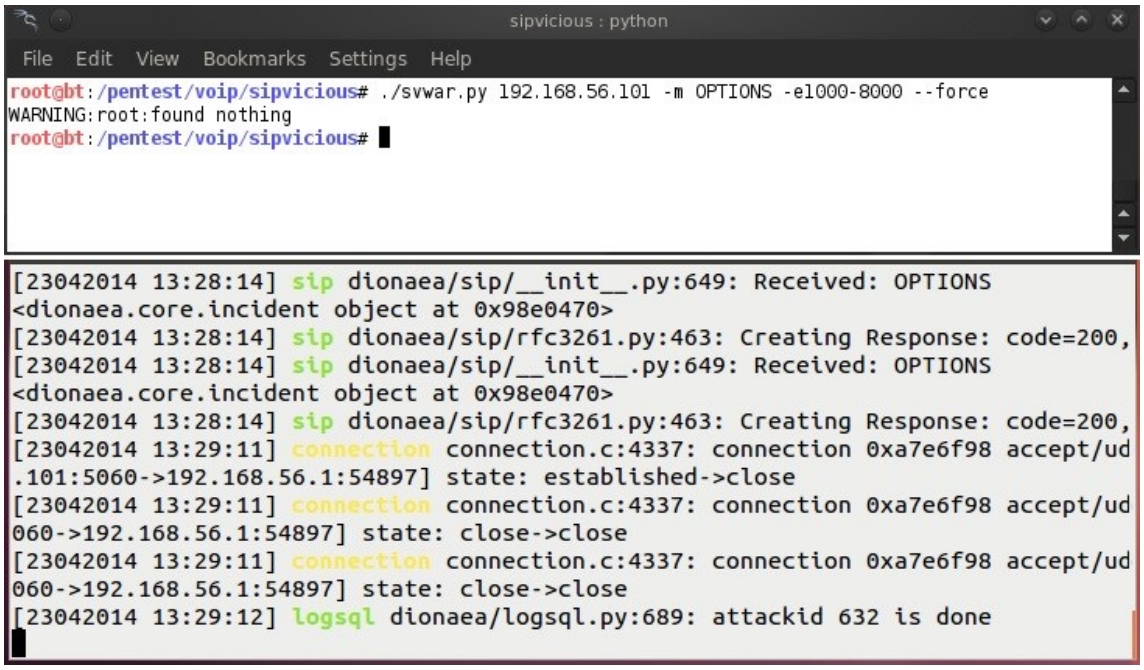
Nástroj SVmap som využila na skenovanie a identifikáciu zariadení na dvoch IP adresách. Na obrázku 5.3 je vidieť, že z prvej IP adresy, na ktorej je spustená Dionaea, SVmap nezískal informácie o zariadení, na rozdiel od druhej adresy, na ktorej honeypot nie je. Útok bol po celú dobu svojho trvania zaznamenávaný produktom Dionaea.

```
root@bt:/pentest/voip/sipvicious# ./svmap.py 192.168.56.101 --fp
| SIP Device          | User Agent | Fingerprint                              |
-------------------------------------------------------------------------------
| 192.168.56.101:5060 | unknown    | Linksys/SPA2102-3.3.6 / 3CXPhoneSystem |

root@bt:/pentest/voip/sipvicious# ./svmap.py 192.168.56.1 --fp
| SIP Device        | User Agent                          | Fingerprint      |
-------------------------------------------------------------------------------
| 192.168.56.1:5060 | Brekeke SIP Server rev.379 Evaluation | AVM or Speedport |
```

Obr. 5.3 Nástroj SVmap

Po spustení nástroja SVwar na skenovanie VoIP zariadení pomocou skúmania získaných SIP odpovedí honeypot Dionaea na zaslané SIP žiadosti odpovedal a celú komunikáciu zaznamenával, no k samotnému nadviazaniu relácie nedošlo. Na obrázku 5.4 je v hornej časti príkazový riadok systému BackTrack, ktorý zobrazuje útok SVwar pomocou metódy OPTIONS. Pod ním sa nachádza výpis honeypotu Dionaea.



Obr. 5.4 SVwar - metóda OPTIONS

5.2.3 **Metasploit**

Modulom Metasploit Enumerator som na objavovanie platných SIP účtov využila metódy REGISTER (táto metóda je preddefinovaná) a OPTIONS. Honeypot, ktorý bol spustený na zadanej cieľovej adrese celú komunikáciu zaznamenával, čo je možné vidieť na obrázku 5.5.

```
[27042014 12:48:57] sip dionaea/sip/__init__.py:649: Received: REGISTER
<dionaea.core.incident object at 0x93fb4c0>
[27042014 12:48:57] sip dionaea/sip/rfc3261.py:463: Creating Response: code=200,
 message=None
[27042014 12:49:07] connection connection.c:4337: connection 0x9384000 accept/ud
p/established [192.168.56.101:5060->192.168.56.1:52761] state: established->clos
e
[27042014 12:49:07] connection connection.c:4337: connection 0x9384000 accept/ud
p/close [192.168.56.101:5060->192.168.56.1:52761] state: close->close
[27042014 12:49:07] connection connection.c:4337: connection 0x9384000 accept/ud
p/close [192.168.56.101:5060->192.168.56.1:52761] state: close->close
[27042014 12:49:07] logsql dionaea/logsql.py:689: attackid 884 is done
```

Obr. 5.5 Metasploit Enumerator - metóda REGISTER

5.3 Výsledky testovania honeypotu Kippo

5.3.1 Nástroj Hping 3

Po zadaní potrebného príkazu a po úspešnom odoslaní požadovaného počtu packetov (v tomto prípade bol útok nastavený na odoslanie štyroch packetov), honeypot Kippo tento útok zaznamenal, ako je možné vidieť na obrázku 5.6.

```
2014-04-26 22:53:17+0200 [kippo.core.honeypot.HoneyPotSSHFactory] New connection
: 192.168.56.1:56685 (192.168.56.101:22) [session: 0]
2014-04-26 22:53:17+0200 [HoneyPotTransport,0,192.168.56.1] connection lost
2014-04-26 22:53:18+0200 [kippo.core.honeypot.HoneyPotSSHFactory] New connection
: 192.168.56.1:56687 (192.168.56.101:22) [session: 1]
2014-04-26 22:53:18+0200 [HoneyPotTransport,1,192.168.56.1] connection lost
2014-04-26 22:53:19+0200 [kippo.core.honeypot.HoneyPotSSHFactory] New connection
```

Obr. 5.6 Nástroj Hping3 – packety zachytené honeypotom

5.3.2 XHydra

Nástroj XHydra na prelomenie užívateľských mien a hesiel pomocou slovníkového útoku nebol schopný v použitom zozname štatisticky najpoužívanejších hesiel nájsť to správne, honeypot Kippo napriek tomu všetky pokusy o prelomenie hesla zaznamenal.

5.3.3 Ncrack

Po zadaní príkazu, v ktorom som zadala ako cieľový port číslo 22 protokolu SSH, sa nástroj pokúsil prelomiť heslo, čo však bolo neúspešné. Honeypot Kippo napriek tomu celú komunikáciu zaznamenal. Časť tejto komunikácie je zobrazená na obrázku 5.7.

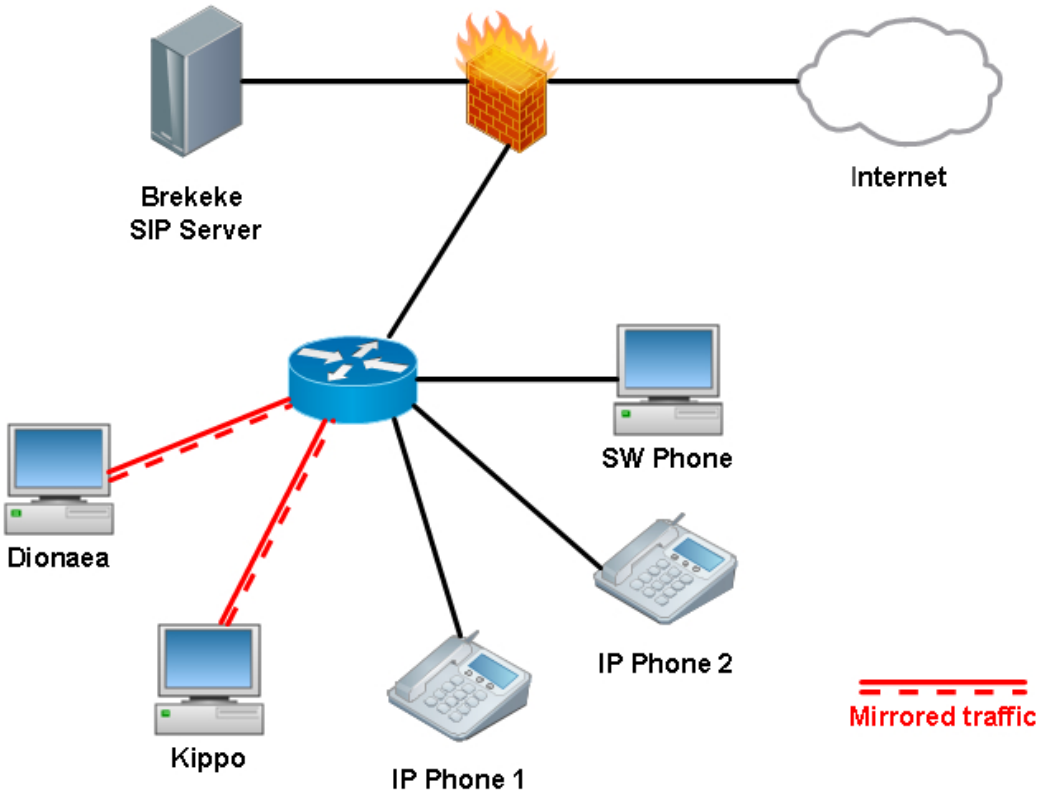
```
2014-04-24 00:29:49+0200 [kippo.core.honeypot.HoneyPotSSHFactory] New connection: 192
.168.56.1:62037 (192.168.56.101:22) [session: 39]
2014-04-24 00:29:49+0200 [HoneyPotTransport,37,192.168.56.1] connection lost
2014-04-24 00:29:49+0200 [HoneyPotTransport,38,192.168.56.1] Remote SSH version: SSH-
2.0-OpenSSH_5.2
2014-04-24 00:29:49+0200 [HoneyPotTransport,38,192.168.56.1] kex alg, key alg: diffie
-hellman-group1-sha1 ssh-rsa
2014-04-24 00:29:49+0200 [HoneyPotTransport,38,192.168.56.1] outgoing: aes128-ctr hma
c-md5 none
2014-04-24 00:29:49+0200 [HoneyPotTransport,38,192.168.56.1] incoming: aes128-ctr hma
c-md5 none
2014-04-24 00:29:49+0200 [HoneyPotTransport,39,192.168.56.1] Remote SSH version: SSH-
2.0-OpenSSH_5.2
2014-04-24 00:29:49+0200 [HoneyPotTransport,39,192.168.56.1] kex alg, key alg: diffie
-hellman-group1-sha1 ssh-rsa
2014-04-24 00:29:49+0200 [HoneyPotTransport,39,192.168.56.1] outgoing: aes128-ctr hma
c-md5 none
2014-04-24 00:29:49+0200 [HoneyPotTransport,39,192.168.56.1] incoming: aes128-ctr hma
c-md5 none
2014-04-24 00:30:09+0200 [HoneyPotTransport,38,192.168.56.1] connection lost
```

Obr. 5.7 Nástroj Ncrack zachytený honeypotom Kippo

5.4 Teoretický návrh využitia vhodného honeypotu v praxi

Po testovaní a analýze vlastností a využiteľnosti vybraných honeypotov v IP telefónii považujem za najvhodnejší nástroj pre využitie v praxi honeypot Dionaea. Zaznamenal všetky použité útoky, reagoval na prichádzajúce SIP správy a celú prevádzku monitoroval. Následne všetky informácie ukladal do databázy, takže bolo možné pomocou vizualizačného nástroja získavať zoznamy útokov, ich priebeh a štatistické grafy. Vybrané zoznamy a grafy budú uvedené v prílohe.

Ideálnym riešením pre nasadenie v praxi by mohla byť kombinácia honeypotov Dionaea a Kippo, kedy by boli okrem SIP útokov monitorované aj SSH služby, prípadne kombinácia spomínaných dvoch honeypotov a SIP servera Brekeke, keďže aj tento server je schopný po správnom nastavení zabrániť niektorým druhom útokov. Na obrázku 5.8 je znázornený návrh takejto siete. Honeypoty Dionaea a Kippo sú v tejto topológii zapojené do mirror portu, takže môžu zaznamenávať celú komunikáciu, ktorá sa bude odohrávať na SIP serveri [19][20][21][22].



Obr. 5.8 Návrh zapojenia honeypotov do siete

Záver

V mojej bakalárskej práci som sa zaoberala problematikou bezpečnostných rizík v IP telefónii a nástrojmi pre realizáciu honeypotov v SIP infraštruktúre. V úvode práce som čitateľa zoznámila so základnými pojmami a protokolmi IP telefónie, ktoré je treba poznať pre hlbšie pochopenie ďalšieho textu. Cieľom druhej kapitoly bolo popísať najvyužívanejšie spôsoby útočenia na VoIP sieť, predovšetkým na protokol SIP. Ďalšia kapitola bola venovaná zoznámeniu sa s pojmom honeypot a s nástrojmi, ktoré sú využívané pre realizáciu honeypotov v prostredí IP telefónie. Následne som popísala nasadenie vybraných honeypotov v SIP infraštruktúre, ich testovanie a využité nástroje. Ďalšia kapitola bola venovaná analýze výsledkov testov. Na základe získaných poznatkov som následne navrhla zapojenie vhodných honeypotov pre využitie v praxi.

Vďaka tejto záverečnej práci som získala väčšie skúsenosti s VoIP technológiou a službami pre zabezpečenie SIP siete, rovnako ako aj s nástrojmi určenými pre Linuxové platformy a v nemalej rade tiež s prácou v samotných Linuxových distribúciách.

Cieľom tejto práce bolo vytvorenie komplexnej analýzy dostupných honeypotov pre IP telefóniu a protokol SIP, ich praktické testovanie a návrh toho najvhodnejšieho pre využitie v praxi. Verím, že práca tento cieľ spĺňa. Napriek tomu je potrebné sa touto problematikou naďalej zaoberať, keďže sa neustále objavujú nové spôsoby, ako na VoIP sieť útočiť.

Použitá literatúra

[1] Miroslav Vozňák, "Spojovací systémy", Vysokoškolské skriptá, VŠB-TU Ostrava, 2012, ISBN 978-80-248-1961-7

[2] Miroslav Vozňák, Filip Řezáč, "Voice over IP", VŠB-TU Ostrava, 2010

[3] Filip Řezáč, "Zabezpečená komunikace na SIP protokolu", Diplomová práca, VŠB-TU Ostrava, 2009

[4] Jakub Šafařík, Filip Řezáč, Miroslav Vozňák "Monitoring of Malicious Traffic in IP Telephony Infrastructure", CESNET z.s.p.o., Praha, 2012

[5] Niels Provos, Thorsten Holz, "Virtual Honeypots: From Botnet Tracking to Intrusion Detection", ISBN: 978-0321336323

[6] Jakub Šafařík, Miroslav Vozňák, Filip Řezáč, Pavol Partila, Karel Tomala, "Automatic Analysis of Attack Data from Distributed Honeypot Network", Ostrava

[7] Lance Spitzner, "Honeypots: Tracking Hackers" ISBN: 978-0321108951

[8] Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard, "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code", ISBN: 978-0-470-61303-0

[9] The Honeynet Project, http://www.honeynet.org/, február 2014

[10] BrekekeWiki, http://www.wiki.brekeke.com/wiki/, marec 2014

[11] Oracle VM VirtualBox, https://www.virtualbox.org /, marec 2014

[12] BackTrack Linux, http://www.backtrack-linux.org/, marec 2014

[13] D. Endler, M. Collier, "Hacking Exposed VoIP", http://hackingvoip.com/, apríl 2014

[14] Wireshark, http://wireshark.org/, marec 2014

[15] Brute Force Lab´s Blog, http://bruteforce.gr/, apríl 2014

[16] I. Ahl, J. Gauthier, "TekDefense", http://tekdefense.com/, apríl 2014

[17] Kippo, SSH honeypot, https://code.google.com/p/kippo/, apríl 2014

[18] Dionaea – catches bugs, http://dionaea.carnivore.it/, apríl 2014

[19] A Virtual Honeypot Framework, https://www.usenix.org/legacy/event/sec04/tech/full_papers/provos/provos_html/honeyd.html/, apríl 2014

[20] Honeypot Concepts, http://www.honeyd.org/concepts.php/, apríl 2014

[21] E. Peter, T. Schiller, "A Practical Guide to Honeypots",
http://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/index.html, apríl 2014

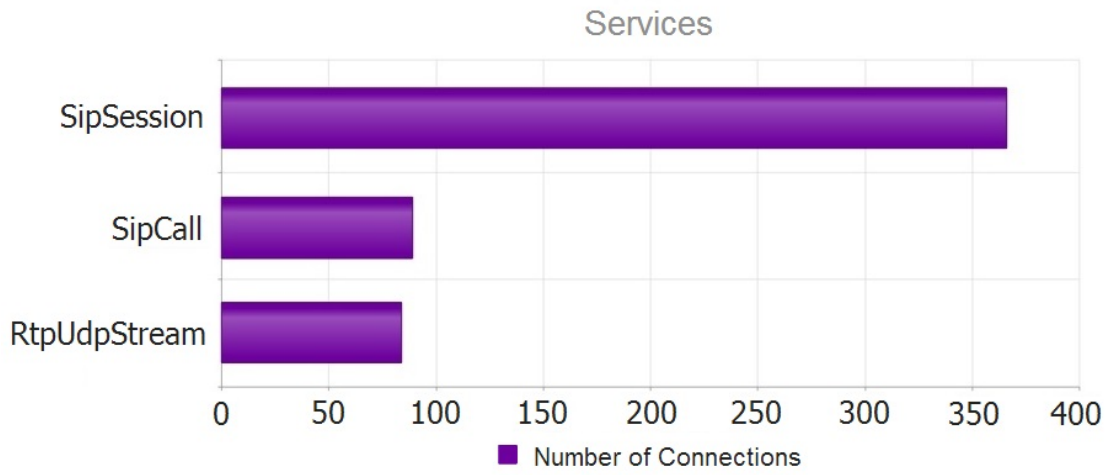
[22] R. Bodó, M. Kostěnec, "Experiences with IDS and Honeypots", March 2012, GN3-NA3-T4-CBPD135

[23] Divya and Sanjeev Kumar, "Analysis of Denial of Service Attackss in IEEE 802.11s Wireless Mesh Networks", India 2009

[24] F.El-moussa, P.Mudhar, A. Jones, "Overview of SIP Attacks and Countermeasures", Edith Cowan University, Perth 2009

Príloha A *Vybrané výstupy z vizualizačného nástroja DionaeaFR: Zoznam zachytených útokov, graf služieb využívaných pri útočení*

ID	State	Protocol	Service	Date	Root	Parent	Sensor	Dst Port	Attacker	Hostname	Src Port
798	connect	udp	SipSession	26-04-2014 22:40:52	798	—	? 192.168.56.101	5060	? 192.168.56.1	—	58962
797	connect	udp	SipSession	26-04-2014 22:35:32	797	—	? 192.168.56.101	5060	? 192.168.56.1	—	64073
796	connect	udp	SipSession	26-04-2014 22:33:10	796	—	? 192.168.56.101	5060	? 192.168.56.1	—	64073
795	connect	udp	SipSession	26-04-2014 22:32:30	795	—	? 192.168.56.101	5060	? 192.168.56.1	—	64073
794	connect	udp	SipSession	26-04-2014 22:31:51	794	—	? 192.168.56.101	5060	? 192.168.56.1	—	64073
793	connect	udp	SipSession	26-04-2014 22:27:40	793	—	? 192.168.56.101	5060	? 192.168.56.1	—	64073
792	connect	udp	SipSession	26-04-2014 22:27:21	792	—	? 192.168.56.101	5060	? 192.168.56.1	—	64073
791	connect	udp	SipSession	26-04-2014 22:26:32	791	—	? 192.168.56.101	5060	? 192.168.56.1	—	64073
790	connect	udp	SipSession	26-04-2014 22:26:22	790	—	? 192.168.56.101	5060	? 192.168.56.1	—	64073
789	connect	udp	SipSession	26-04-2014 22:25:31	789	—	? 192.168.56.101	5060	? 192.168.56.1	—	64073
788	connect	udp	SipSession	26-04-2014 22:24:08	788	—	? 192.168.56.101	5060	? 192.168.56.1	—	64073
787	connect	udp	SipSession	26-04-2014 22:22:55	787	—	? 192.168.56.101	5060	? 192.168.56.1	—	64073
786	connect	udp	SipSession	26-04-2014 22:15:51	786	—	? 192.168.56.101	5060	? 192.168.56.1	—	54167
785	connect	udp	SipSession	26-04-2014 22:15:30	785	—	? 192.168.56.101	5060	? 192.168.56.1	—	54167
784	connect	udp	SipSession	26-04-2014 22:15:17	784	—	? 192.168.56.101	5060	? 192.168.56.1	—	54167


Services
SipSession
SipCall
RtpUdpStream
0
50
100
150
200
250
300
350
400
Number of Connections

Príloha B *CD*

CD obsahuje adresáre:

Text	-Text bakalárskej práce
DionaeaFR	-výstupy z vizualizačného nástroja DionaeaFR (zoznam zachytených útokov)